Data Protection Policy & Procedures

General Data Protection Regulations (2023)

May 2018

Contents

Introduction

Disability Nottinghamshire has always taken seriously its responsibility to look after the information we hold about people, whether that be clients who contact us for help, information and advice, or for volunteers or employees.

On the 25th May 2018, Disability Nottinghamshire will be required to comply with a new General Data Protection Regulations, which will replace the existing Data Protection Act (1998). We have reviewed our current policies and procedures and we will be required to follow new rules, guidance, policies and procedures to comply with these new regulations.

The main principles of GDPR are; lawfulness, fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation and integrity and confidentiality.

The following are the new policies, and procedures and documentation we will follow to meet these principles. They will enable us to comply with the law around data protection, help develop a workplace culture of privacy and security and mean our clients; our employees and volunteers can have confidence that we protect their personal data.

For the purposes of this document;
The Data Controller is: Disability Nottinghamshire (the organisation).
Article 5 (2) of the GDPR requires that:" the controller shall be responsible for, and be able to demonstrate, compliance with the principles."

The Data Protection Officer is:

The Data Processor is: Anyone within the organisation responsible for processing, using, accessing personal data.

The ICO states;
'Controllers are liable for their compliance with the GDPR and must only appoint processors who can provide 'sufficient guarantees' that the requirements of the GDPR will be met and the rights of data subjects protected. In the future, using a processor which adheres to an approved code of conduct or certification scheme may help controllers to satisfy this requirement – though again, no such schemes are currently available'.

'Processors must only act on the documented instructions of a controller. They will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don't comply'.

(Note; at present, Disability Nottinghamshire is in partnership with the D2N2 project. Disability Nottinghamshire uses D2N2 policies and procedures for processing client data for this specific project, and these clients are not considered within the scope of these policies and procedures. Disability Nottinghamshire will not be considered the 'Data Controller' for D2N2 purposes).

Disability Nottinghamshire

Data protection policy
Legal basis for processing data.

The Information Commissioners Office requires Disability Nottinghamshire to identify a legal basis for processing data and information about people.

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on your purpose and relationship with the individual.

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever you process personal data:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.
(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).
(d) Vital interests: the processing is necessary to protect someone's life.
(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.
(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)

Within Disability Nottinghamshire, there are three main types of data subject who have data processed; Employees, Volunteers, and clients.

The Legal basis of processing data for Employees and Volunteers are identified in the contained Asset register, and reasons for identifying this legal basis in the Data Protection policy. These mostly rely on a contractual basis, or a legitimate interest of the organisation.

The ICO state;

"It is likely to be most appropriate where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing.
If you choose to rely on legitimate interests, you take on extra responsibility for ensuring people's rights and interests are fully considered and protected".

When Disability Nottinghamshire rely on Legitimate Interest as a legal basis the DPO Will complete and record a 'Legitimate Interest Assessments (Appendix 2).

The legal basis for processing client data is identified in Asset Register.

Disability Nottinghamshire processes 'sensitive personal data' about clients. Within GDPR this is considered Special Category Data. This data includes a clients; race, ethnic origin, gender, health condition and disabilities.

When identifying a legal basis for processing special category data, the ICO suggests;

"If the information is sensitive personal data, at least one of several other conditions must also be met before the processing can comply with the first data protection principle. These other conditions are as follows.
The individual whom the sensitive personal data is about has given explicit consent to the processing.
The processing is necessary so that you can comply with employment law.
The processing is necessary to protect the vital interests of:
the individual (in a case where the individual's consent cannot be given or reasonably obtained), or
another person (in a case where the individual's consent has been unreasonably withheld)."

With this is mind, Disability Nottinghamshire has identified the legal basis for processing client data as 'Consent'

All consent given from clients to record and process personal data must be recoded.

Disability Nottinghamshire
Information Security Policy

Data Security.

The GDPR requires Disability Nottinghamshire to have policy on keeping data and information secure, destroyed or deleted in a timely manner and breaches of data security recorded and responded to appropriately.
Disability Nottinghamshire will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

Ensuring all paper records are kept in locked storage when not in use. The Office Manager will ensure addition security of Keys and appropriate access.
All access to IT /data bases are password protected. The Office manager will delegate access to password when needed.
The Office Manager will ensure passwords will be changed once per year.
Making sure that, where possible, personal information is pseudonymised or encrypted;
Ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
Ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and
a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Use of email.

‘Personal data’ also includes IP addresses and emails; this will affect responding to enquiries by email.
The amount of personal details, sensitive or confidential information, sent via email should be kept to an absolute minimum. If possible, it’s preferred that you avoid email communication containing this. However, if this is unavoidable and the clients preferred method of communication, please use the encryption instructions below.
If replying to email enquiry, don’t reply by using the ‘Reply’ feature on the email. Your reply will then contain personal data, and we are then responsible for it. Instead, create a new email, replying to the enquiry, by typing in the recipients address (don’t use ‘auto fill’).
Please end the email by pasting;

Disability Nottinghamshire are registered with the Information Commissioner's Office, and will process your personal data in accordance with the General Data Protection Regulation and Data Protection Act 2018. Please refer the Disability Nottinghamshire Privacy Policy for more information on how your personal data will be processed and stored.

When sending any information by email (even with consent to share data) the following process must be followed:

Any confidential of or sensitive personal information that is sent by email must be encrypted. Always send the information to a named person.
Always make sure the recipient knows to expect the email.
Include as little information as possible in the body of the email.
Put the confidential and or sensitive personal information into a document. Encrypt the document by password protecting it. You can then save the document and send to the recipient.
Send the password by another means, either by telephone or SMS

Data Breaches.

A personal data breach means a breach in security leading to the accidental or unlawful loss, alteration, unauthorised disclosure of, access to personal data.
A data breach may take many different forms, for example:

Loss or theft of data or equipment on which personal information is stored;
Unauthorised access to or use of personal information either by a member of staff or third party;
Loss of data resulting from an equipment or systems (including hardware and software) failure;
Human error, such as accidental deletion or alteration of data;
Unforeseen circumstances, such as a fire or flood;
Deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and 'blagging' offences, where information is obtained by deceiving the organisation which holds it.
In the event of a data breach, Disability Nottinghamshire will:
make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

Disability Nottinghamshire

DATA PROTECTION POLICY

(Employees and Volunteers)

You must read this policy because it gives important information about:

- the data protection principles with which the Company must comply;
- what is meant by personal information (or data) and sensitive personal information (or data);
- how we gather, use and (ultimately) delete personal information and sensitive personal information in accordance with the data protection principles;
- where more detailed privacy information can be found, eg about the personal information we gather and use about you, how it is used, stored and transferred, for what purposes, the steps taken to keep that information secure and for how long it is kept;
- your rights and obligations in relation to data protection; and
- the consequences of failure to comply with this policy.

Once you have read and understood this policy, please confirm you that have done so by signing and returning the attached copy to Office Manager.

1 Introduction

1.1 Disability Nottinghamshire keeps and uses personal information (also referred to as data) about job applicants and about current and former employees, temporary and agency workers, contractors, interns, volunteers and apprentices for a number specific lawful purposes.

1.2 This policy sets out how we comply with our data protection obligations and seek to protect personal information relating to our workforce. Its purpose is also to ensure that staff understand and comply with the rules governing the collection, use and deletion of personal information to which they may have access in the course of their work.

1.3 We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information relating to our workforce, and how (and when) we delete that information once it is no longer required.

1.4 **[**The Company's data protection officer, [*insert name*], is responsible for informing and advising the Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with the Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection.

1.5 The office manager is responsible for data protection compliance within the Company. If you have any questions or comments about the content of this policy or if you need further information, you should contact the office manager.

2 Scope

2.1 This policy applies to the personal information of job applicants and current and former staff, including employees, temporary and agency workers, interns, volunteers and apprentices.

2.2 Staff should refer to the Company's [*data protection privacy notice*] and, where appropriate, to its other relevant policies including in relation to [*internet, email and communications, monitoring, social media, information security, data retention, bring your own device (BYOD) and criminal record information*], which contain further information regarding the protection of personal information in those contexts.

2.3 **[**This policy has been drafted with the assistance of a representative group of employees to ensure that it is clear and easy to understand. **]**We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee's contract of employment and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff **[**before OR when**]** it is adopted.

3 Definitions

criminal records information	means personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures;
data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information;
data subject	means the individual to whom the personal information relates;
personal information	(sometimes known as personal data) means information relating to an individual who can be identified (directly or indirectly) from that information;
processing information	means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it;
pseudonymised	means the process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual;
sensitive personal information	(sometimes known as 'special categories of personal data' or 'sensitive personal data') means personal information about an individual's race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual's health, sex life or sexual orientation.

4 Data protection principles

4.1 The Company will comply with the following data protection principles when processing personal information:

4.1.1 we will process personal information lawfully, fairly and in a transparent manner;

4.1.2 we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

4.1.3 we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;

4.1.4 we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information are deleted or corrected without delay;

4.1.5 we will keep personal information**[** in a form which permits identification of data subjects**]** for no longer than is necessary for the purposes for which the information is processed; and

4.1.6 we will take appropriate technical and organisational measures to ensure that personal information are kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

5 Basis for processing personal information

5.1 In relation to any processing activity we will, before the processing starts for the first time, and then regularly while it continues:

5.1.1 review the purposes of the particular processing activity, and select the most appropriate lawful basis (or bases) for that processing, ie:

(a) that the data subject has consented to the processing;

(b) that the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) that the processing is necessary for compliance with a legal obligation to which the Company is subject;

(d) that the processing is necessary for the protection of the vital interests of the data subject or another natural person;**[** or**]**

(e) **[**that the processing is necessary for the performance of a task carried out in the public interest or exercise of official authority; or**]**

(f) that the processing is necessary for the purposes of legitimate interests of the Company or a third party, except where those interests are overridden by the interests of fundamental rights and freedoms of the data subject—see clause 5.2 below.

5.1.2 except where the processing is based on consent, satisfy ourselves that the processing is necessary for the purpose of the relevant lawful basis (ie that there is no other reasonable way to achieve that purpose);

5.1.3 document our decision as to which lawful basis applies, to help demonstrate our compliance with the data protection principles;

5.1.4 include information about both the purposes of the processing and the lawful basis for it in our relevant privacy notice(s);

5.1.5 where sensitive personal information is processed, also identify a lawful special condition for processing that information (see paragraph 6.2.2 below), and document it; and

5.1.6 where criminal offence information is processed, also identify a lawful condition for processing that information, and document it.

5.2 When determining whether the Company's legitimate interests are the most appropriate basis for lawful processing, we will:

5.2.1 conduct a legitimate interests assessment (LIA) and keep a record of it, to ensure that we can justify our decision;

5.2.2 if the LIA identifies a significant privacy impact, consider whether we also need to conduct a data protection impact assessment (DPIA);

5.2.3 keep the LIA under review, and repeat it if circumstances change; and

5.2.4 include information about our legitimate interests in our relevant privacy notice(s).

6 Sensitive personal information

6.1 Sensitive personal information is sometimes referred to as 'special categories of personal data' or 'sensitive personal data'.

6.2 The Company may from time to time need to process sensitive personal information. We will only process sensitive personal information if:

6.2.1 we have a lawful basis for doing so as set out in paragraph 5.1.1 above, eg it is necessary for the performance of the employment contract, to comply with the Company's legal obligations or for the purposes of the Company's legitimate interests; and

6.2.2 one of the special conditions for processing sensitive personal information applies, eg:

(a) the data subject has given has given explicit consent;

(b) the processing is necessary for the purposes of exercising the employment law rights or obligations of the Company or the data subject;

(c) the processing is necessary to protect the data subject's vital interests, and the data subject is physically incapable of giving consent;

(d) processing relates to personal data which are manifestly made public by the data subject;

(e) the processing is necessary for the establishment, exercise or defence of legal claims; or

(f) the processing is necessary for reasons of substantial public interest.

6.3 Before processing any sensitive personal information, staff must notify **[**the data protection officer OR [*insert job title or department*]**]** of the proposed processing, in order that **[**the data protection officer OR [*insert job title or department*]**]** may assess whether the processing complies with the criteria noted above.

6.4 Sensitive personal information will not be processed until:

6.4.1 the assessment referred to in paragraph 6.3 has taken place; and

6.4.2 the individual has been properly informed (by way of a privacy notice or otherwise) of the nature of the processing, the purposes for which it is being carried out and the legal basis for it.

6.5 **[**The Company will not carry out automated decision-making (including profiling) based on any individual's sensitive personal information.**]**

6.6 The Company's [*data protection privacy notice*] sets out the types of sensitive personal information that the Company processes, what it is used for and the lawful basis for the processing.

6.7 In relation to sensitive personal information, the Company will comply with the procedures set out in paragraphs 6.8 and 6.9 below to make sure that it complies with the data protection principles set out in paragraph 4 above.

6.8 **During the recruitment process**: the HR department, with guidance from **[**the data protection officer OR [*insert job title or department*]**]**, will ensure that (except where the law permits otherwise):

6.8.1 during the short-listing, interview and decision-making stages, no questions are asked relating to sensitive personal information, eg race or ethnic origin, trade union membership or health;

6.8.2 if sensitive personal information is received, eg the applicant provides it without being asked for it within his or her CV or during the interview, no record is kept of it and any reference to it is immediately deleted or redacted;

6.8.3 any completed equal opportunities monitoring form is kept separate from the individual's application form, and not be seen by the person shortlisting, interviewing or making the recruitment decision;

6.8.4 'right to work' checks are carried out before an offer of employment is made unconditional, and not during the earlier short-listing, interview or decision-making stages;

6.8.5 we will **[**not ask health questions in connection with recruitment OR only ask health questions once an offer of employment has been made**]**.

6.9 **During employment**: the HR department, with guidance from the **[**data protection officer OR Office Manager will process:

6.9.1 health information for the purposes of administering sick pay, keeping sickness absence records, monitoring staff attendance and facilitating employment-related health and sickness benefits;

6.9.2 sensitive personal information for the purposes of equal opportunities monitoring and pay equality reporting**[**. Where possible, this information will be anonymised**]**; and

6.9.3 trade union membership information for the purposes of staff administration and administering 'check off'.

7 Criminal records information

Criminal records information will be processed in accordance with the Company's guidelines for processing special category data.

8 Data protection impact assessments (DPIAs)

8.1 Where processing is likely to result in a high risk to an individual's data protection rights (eg where the Company is planning to use a new form of technology), we will, before commencing the processing, carry out a DPIA to assess:

8.1.1 whether the processing is necessary and proportionate in relation to its purpose;

8.1.2 the risks to individuals; and

8.1.3 what measures can be put in place to address those risks and protect personal information.

8.2 Before any new form of technology is introduced, the manager responsible should therefore contact **[**the data protection officer OR [*insert job title or department*]**]** in order that a DPIA can be carried out.

8.3 During the course of any DPIA, the employer will seek the advice of the **[**data protection officer OR [*insert job title or department*]**]** and the views of**[** a representative group of**]** employees and any other relevant stakeholders.

9 Documentation and records

9.1 We will keep written records of processing activities**[** which are high risk, ie which may result in a risk to individuals' rights and freedoms or involve sensitive personal information or criminal records information**]**, including:

9.1.1 the name and details of the employer's organisation (and where applicable, of other controllers, the employer's representative and DPO);

9.1.2 the purposes of the processing;

9.1.3 a description of the categories of individuals and categories of personal data;

9.1.4 categories of recipients of personal data;

9.1.5 **[**where relevant, details of transfers to third countries, including documentation of the transfer mechanism safeguards in place;**]**

9.1.6 where possible, retention schedules; and

9.1.7 where possible, a description of technical and organisational security measures.

9.2 As part of our record of processing activities we document, or link to documentation, on:

9.2.1 information required for privacy notices;

9.2.2 records of consent;

9.2.3 controller-processor contracts;

9.2.4 the location of personal information;

9.2.5 DPIAs; and

9.2.6 records of data breaches.

9.3 If we process sensitive personal information or criminal records information, we will keep written records of:

9.3.1 the relevant purpose(s) for which the processing takes place, including (where required) why it is necessary for that purpose;

9.3.2 the lawful basis for our processing; and

9.3.3 whether we retain and erase the personal information in accordance with our policy document and, if not, the reasons for not following our policy.

9.4 We will conduct regular reviews of the personal information we process and update our documentation accordingly.**[** This may include:**]**

9.4.1 **[**carrying out information audits to find out what personal information the Company holds;

9.4.2 distributing questionnaires and talking to staff across the Company to get a more complete picture of our processing activities; and

9.4.3 reviewing our policies, procedures, contracts and agreements to address areas such as retention, security and data sharing.**]**

9.5 **[**We document our processing activities in electronic form so we can add, remove and amend information easily.**]**

10 Privacy notice

10.1 The Company will issue privacy notices from time to time, informing you about the personal information that we collect and hold relating to you, how you can expect your personal information to be used and for what purposes.

10.2 We will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

11 Individual rights

11.1 You (in common with other data subjects) have the following rights in relation to your personal information:

11.1.1 to be informed about how, why and on what basis that information is processed—see the Company's [*data protection privacy notice*];

11.1.2 to obtain confirmation that your information is being processed and to obtain access to it and certain other information, by making a subject access request.

11.1.3 to have data corrected if it is inaccurate or incomplete;

11.1.4 to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed, or if there are no overriding legitimate grounds for the processing (this is sometimes known as 'the right to be forgotten');

11.1.5 to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the employer no longer needs the personal information but you require the data to establish, exercise or defend a legal claim; and

11.1.6 to restrict the processing of personal information temporarily where you do not think it is accurate (and the employer is verifying whether it is accurate), or where you have objected to the processing (and the employer is considering whether the organisation's legitimate grounds override your interests).

11.2 If you wish to exercise any of the rights in paragraphs 11.1.3 to 11.1.6, please contact **[**the data protection officer OR [*insert job title or department*]**]**.

12 Individual obligations

12.1 Individuals are responsible for helping the Company keep their personal information up to date. You should let [*the HR department*] know if the information you have provided to the Company changes, for example if you move house or change details of the bank or building society account to which you are paid.**[** Alternatively, you can update your own personal information on a secure basis via the Company's intranet.**]**

12.2 You may have access to the personal information of other members of staff, suppliers and **[**customers OR clients**]** of the Company in the course of your employment or engagement. If so, the Company expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 11.1 above.

12.3 If you have access to personal information, you must:

12.3.1 only access the personal information that you have authority to access, and only for authorised purposes;

12.3.2 only allow other Company staff to access personal information if they have appropriate authorisation;

12.3.3 only allow individuals who are not Company staff to access personal information if you have specific authority to do so from **[**the data protection officer OR [*insert job title or department*]**]**;

12.3.4 keep personal information secure (eg by complying with rules on access to premises, computer access, password protection and secure file storage and destruction and other precautions set out in the Company's [*information security policy*]);

12.3.5 not remove personal information, or devices containing personal information (or which can be used to access it), from the Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and

12.3.6 not store personal information on local drives or on personal devices that are used for work purposes.

12.4 You should contact **[**the data protection officer OR [*insert job title or department*]**]** if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):

12.4.1 processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the conditions in paragraph 6.2.2 being met;

12.4.2 any data breach as set out in paragraph 15.1 below;

12.4.3 access to personal information without the proper authorisation;

12.4.4 personal information not kept or deleted securely;

12.4.5 removal of personal information, or devices containing personal information (or which can be used to access it), from the Company's premises without appropriate security measures being in place;

12.4.6 any other breach of this Policy or of any of the data protection principles set out in paragraph 4.1 above.

13 Information security

13.1 The Company will use appropriate technical and organisational measures**[** in accordance with the Company's **[**policies OR information security policy**]]** to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. These may include:

13.1.1 making sure that, where possible, personal information is pseudonymised or encrypted;

13.1.2 ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

13.1.3 ensuring that, in the event of a physical or technical incident, availability and access to personal information can be restored in a timely manner; and

13.1.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13.2 Where the Company uses external organisations to process personal information on its behalf, additional security arrangements need to be implemented in contracts with those organisations to safeguard the security of personal information. In particular, contracts with external organisations must provide that:

13.2.1 the organisation may act only on the written instructions of the Company;

13.2.2 those processing the data are subject to a duty of confidence;

13.2.3 appropriate measures are taken to ensure the security of processing;

13.2.4 sub-contractors are only engaged with the prior consent of the Company and under a written contract;

13.2.5 the organisation will assist the Company in providing subject access and allowing individuals to exercise their rights under the GDPR;

13.2.6 the organisation will assist the Company in meeting its GDPR obligations in relation to the security of processing, the notification of data breaches and data protection impact assessments;

13.2.7 the organisation will delete or return all personal information to the Company as requested at the end of the contract; and

13.2.8 the organisation will submit to audits and inspections, provide the Company with whatever information it needs to ensure that they are both meeting their data protection obligations, and tell the Company immediately if it is asked to do something infringing data protection law.

13.3 Before any new agreement involving the processing of personal information by an external organisation is entered into, or an existing agreement is altered, the relevant

staff must seek approval of its terms by the **[**data protection officer OR [*insert job title or department*]**]**.

14 Storage and retention of personal information

14.1 Personal information (and sensitive personal information) will be kept securely in accordance with the Company's [*information security policy*].

14.2 Personal information (and sensitive personal information) should not be retained for any longer than necessary. The length of time over which data should be retained will depend upon the circumstances, including the reasons why the personal information was obtained.**[** Staff should follow the Company's [*records retention policy*] which set out the relevant retention period, or the criteria that should be used to determine the retention period.**]** Where there is any uncertainty, staff should consult **[**the data protection officer OR [*insert job title or department*]**]**.

14.3 Personal information (and sensitive personal information) that is no longer required will be deleted permanently from our information systems and any hard copies will be destroyed securely.

15 Data breaches

15.1 A data breach may take many different forms, for example:

15.1.1 loss or theft of data or equipment on which personal information is stored;

15.1.2 unauthorised access to or use of personal information either by a member of staff or third party;

15.1.3 loss of data resulting from an equipment or systems (including hardware and software) failure;

15.1.4 human error, such as accidental deletion or alteration of data;

15.1.5 unforeseen circumstances, such as a fire or flood;

15.1.6 deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and

15.1.7 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

15.2 The Company will:

15.2.1 make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and

15.2.2 notify the affected individuals, if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

16 International transfers

16.1 **[**The Company will not transfer personal information outside the European Economic Area (EEA), which comprises the countries in the European Union and Iceland, Liechtenstein and Norway.

OR

16.2 The Company may transfer personal information outside the European Economic Area (EEA) (which comprises the countries in the European Union and Iceland, Liechtenstein and Norway) to [*insert name of country*] on the basis **[**that that country, territory or organisation is designated as having an adequate level of protection OR that the organisation receiving the information has provided adequate safeguards by way of **[**binding corporate rules OR standard data protection clauses OR of compliance with an approved code of conduct**]].]**

17 Training

The Company will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

18 Consequences of failing to comply

18.1 The Company takes compliance with this policy very seriously. Failure to comply with the policy:

18.1.1 puts at risk the individuals whose personal information is being processed; and

18.1.2 carries the risk of significant civil and criminal sanctions for the individual and the Company; and

18.1.3 may, in some circumstances, amount to a criminal offence by the individual.

18.2 Because of the importance of this policy, an employee's failure to comply with any requirement of it may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

18.3 If you have any questions or concerns about anything in this policy, do not hesitate to contact **[**the data protection officer OR [*insert job title or department*]**]**.

I have read and understood this policy and agree to abide by its terms.

Signed.....

Disability Nottinghamshire

Data Asset Register

Data Asset name / category	**Description of asset**	**Is data shared?**	**How is the data stored / secured**	**Purpose of processing data**	**Legal basis for processing data.**	**DPIA required**?
Client record	See 'Client Details Form' All contact and actions for / with client	No	IT and paper IT password protection. Paper, locked storage.	1) To enable service delivery to client. 2) Statistics for funding. 3) Management performance / quality monitoring.	Presently 'implied consent' May2018; 'explicit consent'	Yes
Employment application and employment contract details.	See Employment privacy notice. Including contract of employment.	Yes	Paper, locked storage	Legal and contractual requirement.	Necessity to perform a contract.	No
Payroll and pension	Payments made pension contributions.	Yes	Electronic, password protected	Staff payments and pension contributions are made	Legal and contractual requirement	No.
Accident records	Personal details of anyone involved in accident at work	Yes H&S executive.	Paper /email Locked storage. Password protection	Health and safety requirements. Monitoring of safe environment.	Legal and contractual requirement	No
Staff performance records	Training, supervision, appraisals	No	Paper, locked storage	Support staff and service development	Legitimate interest	No

Disability Nottinghamshire
Data Retention schedule

One of the six main principles of GDPR regards 'STORAGE LIMITATION'.
Regulations advise that 'personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary'.
Where not subject to any further contractual or legal constraints, personal data shall be deleted/ disposed of, after these periods.

GDPR does not specify lengths of time to keep data. These periods are based on an assessment of a reasonable period for purposes required.
Any data of data recording not referred to here should be referred to the Data Protection Officer.

The [insert job title] shall be responsible for the secure deletion / destruction of records in line with this schedule.

Description of data record.	**Retention Period.**
Client records that have been subject to complaints or disputes or legal action.	16 years
Client records other than above.	6 years
Personnel files of employees and volunteers.	6 years (from end of employment)
Payroll records, income tax, NI records and HMRC correspondence.	3 years
SSPI records.	3 months.
Pension entitlement / contribution history	As long as there is a member or dependent liability
DBS check for employees and volunteers	6 years.
Medical records for C.O.H.S (1999)	40 years
Accident book	3 years
Risk assessments	40 years
Contractual records	6 years
Summary of record of service (name, position etc)	10 years
Accident or injury at work records	12 years
Job Applications/ CV's	1 year
Staff and volunteer references	1 year

Disability Nottinghamshire
Privacy Notices for clients/ guidance.

Under GDPR, Disability Nottinghamshire must inform people how we collect and use their information - the best way to do this is in a privacy notice. This should be available in a number of formats such as on your website, or in paper format.

Communicating privacy information

You can provide privacy notices through a variety of media:

Orally - face to face or when you speak to someone on the telephone (it's a good idea to document this).

In writing - printed media; printed adverts; forms, such as financial applications or job application forms.

Through signage - for example an information poster in a public area.

Electronically - in text messages; on websites; in emails; in mobile apps.

It is good practice to use the same medium you use to collect personal information to deliver privacy notices. So, if you are collecting information through an online form you should provide a just-in-time notice as the individual fills out the form. It would not be good practice to collect information through the form and then email the individual with a separate link to a privacy notice.

In some contexts it can be very difficult to communicate a privacy notice. For example, in an emergency situation obtaining personal details quickly can be critical to protecting an individual. In cases like these, you should explain how you use the information at an appropriate point later on, or if you can't provide privacy information, it is particularly important to make sure you only use the information you collect in a way that members of the public are likely to anticipate and agree to.

Communicating Privacy Notices.

Disability Nottinghamshire will use a range of methods of providing privacy notices to clients, referred to by the ICO as a layered approach;

Layered approach

A layered approach can be useful as it allows you to provide the key privacy information immediately and have more detailed information available elsewhere for those that want it. This is used where there is not enough space to provide more detail or if you need to explain a particularly complicated information system to people.

Just in time notices

Just-in-time notices are a tool you can use to provide relevant and focused privacy information in such situations. This is another type of layered approach to provide information at certain points of data collection.

An example of a 'Just in time notice' for a telephone enquiry may be;

"*We need to collect some information from you so we can best help with your enquiry. You don't need to tell us any personal details if you choose not to. If you do, we will keep this information safe and confidential. We won't share the information we have about you with anyone outside of Disability Nottinghamshire without your approval. We sometimes use statistics to help us get funding; these do not contain your personal details. Are you happy to give your consent to keeping this information?"* **Record consent given.**

"If you want to know more about how and why we collect this information, and your rights around this, you can visit our website, or if you don't have access to a computer, you can speak to a member of our team about your rights in this area".

The GDPR states that consent must be freely given, specific, informed and unambiguous.
Disability Nottinghamshire works with many clients with learning Disabilities, or other disabilities that mean accessing written or verbal communication can present challenges.
With this in mind Disability Nottinghamshire will develop and 'Easy Read / Accessible' privacy notice for all clients to have access to information about their rights around data protection (See Appendix 5).

Privacy Notice for clients

Permission to use your personal data.

At Disability Nottinghamshire we collect and use your personal information so we can best help with your enquiry
We have to ask for your permission to record and use your personal information. We can still help with your enquiry if you don't want to give us your permission, but it might limit us in what we can do to help.

Your consent to record this information is our legal basis for doing so.

We only ask for the information we need. We always let you decide what you're comfortable telling us, explain why we need it and treat it as confidential, safe and secure.

When we record and use your personal information we only access it when we have a good reason, we won't share it with anyone outside of Disability Nottinghamshire without your permission, and we don't sell it to commercial organisations

If we ever did need to use or share your information without your permission, we'll always make sure there's a legal basis for it. Situations where we might have to use or share your information include:

To comply with the law - for example, if a court orders us to share information. This is called 'legal obligation'

To protect someone's life - for example, sharing information with a paramedic if a client was unwell at our office. This is called 'vital interests'

To carry out our legitimate aims and goals as a charity - for example, to create statistics for our national research. This is called 'legitimate interests'

To defend our legal rights - for example, sharing information with our legal advisors if there was a complaint that we gave the wrong advice or information.

We handle and store your personal information in line with the law - including the General Data Protection Regulation.

Working on your behalf

When you give us authority to act on your behalf, for example to help you with a welfare benefits claim, we might need to share information with that third party, for example the DWP. We would always ask for extra permission before we did this and explain why we might need to do this.

Keeping your personal information safe and secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

Use of emails and Disability Nottinghamshire Social Media

If you email us we may need to keep a record of your contact and your email address and the email. For security reasons we will not include any confidential information about you in any email we send to you, unless you agree to this, and we will then make sure any sensitive personal information is encrypted.

We suggest that you keep the amount of confidential information you send to us via email to a minimum and use email encryption where possible.

When you interact with us on social media platforms such as Facebook, WhatsApp, Twitter or LinkedIn, we may also obtain some personal information about you.

If you engage with us by social media, we will not store or process your personal details, other than for statistical purposes.

The information we receive will depend on the privacy preferences you have set on each platform and the privacy policies of each platform. To change your settings on these platforms, please refer to their privacy notices.

Your rights

You have the right to object to us keeping information about you. You have the right to access this information we keep, to correct it if it's wrong. In some cases you have to right to have this information deleted.
When you request access to your personal data, we will normally provide this free of charge, and provide it within one month of request.

You can contact us for further information

If you have any questions about how your information is collected or used, you can contact our office.
You can find out what personal information we hold about you.
You can correct your information if it's wrong, out of date or incomplete
You can request we delete your information
You can ask us to limit what we do with your data - for example, ask us not to share it if you haven't asked us already
You can ask us to give you a copy of the data we hold in a format you can use to transfer it to another service
You can ask us stop using your information

You can contact us at:

Disability Nottinghamshire
Room 6, Park Road Resource Centre, 53 Park Road,
Mansfield Woodhouse NG19 8ER
Telephone: 01623658060
Email: **advice@disabilitynottinghamshire.org.uk**

How to complain

We hope that we can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint

You can get more information about your rights on the Information Commissioners website.

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

Disability Nottinghamshire

Data protection privacy notice (employment)

This notice explains what personal data (information) we hold about you, how we collect it, and how we use and may share information about you during your employment and after it ends. We are required to notify you of this information under data protection legislation. Please ensure that you read this notice (sometimes referred to as a 'privacy notice') and any other similar notice we may provide to you from time to time when we collect or process personal information about you.

Who collects the information

Disability Nottinghamshire is a 'data controller' and gathers and uses certain information about you and so, in this notice, references to 'we' or 'us' mean the Company and our group companies.**]**

Data protection principles

We will comply with the data protection principles when gathering and using personal information, as set out in our [*data protection (employment) policy*].

[About the information we collect and hold (Option 1)

What information

We may collect the following information during your employment:

- Your name, contact details (ie address, home and mobile phone numbers, email address) and emergency contacts (ie name, relationship and home and mobile phone numbers);
- Information collected during the recruitment process that we retain during your employment;
- Employment contract information;
- Details of salary and benefits, bank/building society, National Insurance and tax information, your age;
- Details of your spouse/partner and any dependants;
- Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information;
- **[**A copy of your driving licence;**]**
- **[**Details of your share incentive arrangements, and all information included in these and necessary to implement and administer them;**]**
- Details of your pension arrangements, and all information included in these and necessary to implement and administer them;
- Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health);
- Your racial or ethnic origin, sex and sexual orientation, religious or similar beliefs;

- **[**Criminal records information, including the results of Disclosure and Barring Service (DBS) checks;**]**
- **[**Your trade union membership;**]**
- Information on grievances raised by or involving you;
- Information on conduct and/or other disciplinary issues involving you;
- Details of your appraisals and performance reviews;
- Details of your performance management/improvement plans (if any);
- Details of your time and attendance records;
- **[**Information regarding your work output;**]**
- Information in applications you make for other positions within our organisation;
- Information about your use of our IT, communication and other systems, and other monitoring information;
- Details of your use of business-related social media, such as LinkedIn;
- Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur); and
- Details in references about you that we give to others.

Certain of the categories above may not apply to you if you are a**[**n**] [**worker, **][**agency worker, **][**independent contractor, **][**freelancer, **][**volunteer **][**intern**]**.

How we collect the information

We may collect this information from you, your personnel records, the Home Office, **[**share scheme administrators, **][**pension administrators, **]**your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators, **[**the DBS, **][**your trade union, **]**other employees, **[**consultants and other professionals we may engage, eg to advise us generally and/or in relation to any grievance, conduct appraisal or performance review procedure,**] [**[*insert details of systems used eg door entry systems, swipe card systems, time management system, time clock records, application logs*], **][**[*insert details of relevant systems, such as keystrokes and mouse movements, screen capture, application logs, webcams*], **][**automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote access systems,**[** trading platforms,**]** email and instant messaging systems, intranet and Internet facilities, telephones, voicemail, mobile phone records [*insert any other relevant systems such as data loss prevention tools, next-generation firewalls, unified threat management systems, transport layer security, eDiscovery technology, mobile device management systems*], **][**relevant websites and applications**]**.

Why we collect the information and how we use it

We will typically collect and use this information for the following purposes (other purposes that may also apply are explained in our [*set out details, eg data protection policy*]):

- for the performance of a contract with you, or to take steps to enter into a contract;
- for compliance with a legal obligation (eg our obligations to you as your employer under employment protection and health safety legislation, and under statutory codes of practice, such as those issued by Acas); and
- for the purposes of our legitimate interests or those of a third party (such as a benefits provider), but only if these are not overridden by your interests, rights or freedoms.

Further information on the monitoring we undertake in the workplace and how we do this is available by speaking with the Office Manager.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any material changes to information we collect or to the purposes for which we collect and process it.

How we may share the information

We may also need to share some of the above categories of personal information with other parties, such as external contractors and our professional advisers and with potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information **[**with our regulators or **]**as required to comply with the law.

OR

About the information we collect and hold (Option 2)

The table set out in the Schedule summarises the information we collect and hold, how and why we do so, how we use it and with whom it may be shared.

We may also need to share some of the categories of personal information set out in the Schedule with other parties, such as external contractors and our professional advisers and potential purchasers of some or all of our business or on a re-structuring. Usually, information will be anonymised but this may not always be possible. The recipient of the information will be bound by confidentiality obligations. We may also be required to share some personal information **[**with our regulators or **]**as required to comply with the law.

We seek to ensure that our information collection and processing is always proportionate. We will notify you of any changes to information we collect or to the purposes for which we collect and process it.**]**

Where information may be held

Information may be held at our offices and those of our group companies, and third party agencies, service providers, representatives and agents as described above. We have security measures in place to seek to ensure that there is appropriate security for information we hold**[** including those measures detailed in our information security policy.

How long we keep your information

We keep your information during and after your employment for no longer than is necessary for the purposes for which the personal information is processed.[Further details on this are available in our data retention schedule.

Your rights to correct and access your information and to ask for it to be erased

Please contact [our Data Protection Officer (DPO) [*insert name*] OR [*insert name*]] who can be contacted [*set out details of how DPO/named person can be contacted, eg email and telephone number*] if (in accordance with applicable law) you would like to correct or request access to information that we hold relating to you or if you have any questions about this notice. You also have the right to ask our Data Protection Officer OR [*insert name*] OR for some but not all of the information we hold and process to be erased (the 'right to be forgotten') in certain circumstances. [Our Data Protection Officer OR [*insert name*]] will provide you with further information about the right to be forgotten, if you ask for it.

Keeping your personal information secure

We have appropriate security measures in place to prevent personal information from being accidentally lost, or used or accessed in an unauthorised way. We limit access to your personal information to those who have a genuine business need to know it. Those processing your information will do so only in an authorised manner and are subject to a duty of confidentiality.

We also have procedures in place to deal with any suspected data security breach. We will notify you and any applicable regulator of a suspected data security breach where we are legally required to do so.

How to complain

We hope that [our Data Protection Officer OR [*insert name*]] can resolve any query or concern you raise about our use of your information. If not, contact the Information Commissioner at ico.org.uk/concerns/ or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

The information we collect	**How we collect the information**	**Why we collect the information**	**How we use and may share the information**
Your name, contact details (ie address, home and mobile phone numbers, email address) and emergency contacts (ie name, relationship and home and mobile phone numbers) ☐	From you	To enter into/perform the employment contract Legitimate interest: to maintain employment records and good employment practice	To enter into/perform the employment contract
Details of salary and benefits, bank/building society, National Insurance and tax information, your age ☐	From you	To perform the employment contract including payment of salary and benefits Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To ensure you receive the correct pay and benefits Information shared with our payroll administrators [*insert name*] and with HM Revenue & Customs (HMRC)
Details of your spouse/partner and any dependants ☐	From you	To perform the employment contract including employment-related benefits, eg private medical insurance, life assurance and pension	To ensure you receive the correct pay and benefits Information shared with our payroll administrators [*insert name*] and with HM Revenue & Customs (HMRC)

Your nationality and immigration status and information from related documents, such as your passport or other identification and immigration information ☐	From you and, where necessary, the Home Office	To enter into/perform the employment contract To comply with our legal obligations Legitimate interest: to maintain employment records	To carry out right to work checks Information may be shared with the Home Office
[A copy of your driving licence ☐]	**[**From you**]**	**[**To perform the employment contract**]** **[**To comply with our legal obligations**]** **[**To comply with the terms of our insurance**]**	**[**To ensure that you have a clean driving licence**]** **[**Information may be shared with our insurer**]**
Details of your share incentive arrangements, and all information included in these and necessary to implement and administer them ☐	From you, our share scheme administrators [*insert name*] and your personnel records	To perform the share incentive contract Legitimate interests: to comply with tax, legal, regulatory and corporate governance obligations and good employment practice, to carry out obligations under employment law, for the establishment, exercise or defence of legal claims, to incentivise staff	To administer your share scheme benefits Information shared with our share scheme administrators [*insert name*]**[**, with trustees of the [*insert name*] employee benefit trust**]**, with HMRC and with any third party granting or satisfying the share incentive arrangements
Details of your pension arrangements, and all information included in these and necessary to implement and administer them ☐	From you, from our pension administrators [*insert name*] and (where necessary) from your own pension fund administrators	To perform the employment contract including employment-related benefits To comply with our legal	**[**To administer your pension benefits AND/OR To comply with our auto-enrolment

		obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	pension obligations**]** Information shared with our pension administrators [*insert name*] and with HMRC
Information in your sickness and absence records (including sensitive personal information regarding your physical and/or mental health) ☐	From you, from your doctors, from medical and occupational health professionals we engage and from our insurance benefit administrators [*insert name*]	To perform the employment contract including employment-related benefits To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	To maintain employment records, to administer sick pay entitlement, to follow our policies and to facilitate employment-related health and sickness benefits To comply with our legal obligations to you as your employer Information shared with your doctors, with medical and occupational health professionals we engage and with our insurance benefit administrators [*insert name*] For further information, see ***** below
Your racial or ethnic origin, sex and sexual orientation, religious or	From you	To comply with our legal obligations and	To comply with our equal opportunities

similar beliefs		for reasons of substantial public interest**[** (equality of opportunity or treatment)**]**	monitoring obligations and to follow our policies For further information, see ***** below
Criminal records information, including the results of Disclosure and Barring Service (DBS) checks ☐	From you and the DBS	To perform the employment contract To comply with our legal obligations For reasons of substantial public interest**[** (preventing or detecting unlawful acts,**[** suspicion of terrorist financing or money laundering in the regulated sector**]** and protecting the public against dishonesty)**]**	To carry out statutory checks Information shared with DBS and other regulatory authorities as required For further information, see ***** below
[Your trade union membership**]**	**[**From you or your trade union**]**	**[**To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice**]**	**[**For staff administration and to pay trade union premiums and register the status of a protected employee Information shared with your trade union For further information, see ***** below**]**
Information on grievances raised by or involving you	From you, from other employees and from consultants we may engage in relation to	To perform the employment contract To comply with	For staff administration, to follow our policies and to

	the grievance procedure	our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	deal with grievance matters Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]**
Information on conduct issues involving you	From you, from other employees and from consultants we may engage in relation to the conduct procedure	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and to deal with disciplinary and grievance matters Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]**
Details of your appraisals and performance reviews	From you, from other employees **[**and from consultants we may engage in relation to the appraisal/performance review process**]**	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to	For staff administration and assessments, to follow our policies, to monitor staff performance and conduct and to deal with disciplinary and grievance matters Information

		ensure safe working practices	shared with relevant managers, HR personnel **[**and with consultants we may engage**]**
Details of your performance management/improvement plans (if any)	From you, from other employees **[**and from consultants we may engage in relation to the performance review process**]**	To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice, to ensure safe working practices	For staff administration and assessments, to follow our policies and to monitor staff performance Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]**
Details of your time and attendance records	From you **[**and from [*insert details of systems used eg door entry systems, swipe card systems, time management system, time clock records, application logs*]**]**	To perform the employment contract Legitimate interest: to monitor and manage staff access to our systems and facilities and to record staff absences	For payroll and staff administration and assessments, to follow our policies and to monitor staff performance and attendance Information shared with relevant managers, HR personnel **[**and with consultants we may engage**][** and with our payroll administrators [*insert name*]**]**
[Information regarding your work output]	**[**[*Insert details of relevant systems, such as keystrokes and mouse movements, screen capture,*	**[**To perform the employment contract Legitimate	**[**For payroll and staff administration and assessments, to

	application logs, webcams]**]**	interests: to maintain employment records**]**	follow our policies and to monitor staff performance and attendance Information shared with relevant managers, HR personnel **[**and with consultants we may engage**][** and with our payroll administrators [*insert name*]**]]**
Information in applications you make for other positions within our organisation	From you	To enter into/perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To process the application Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]**
Information about your use of our IT, communication and other systems	Automated monitoring of our websites and other technical systems, such as our computer networks and connections, CCTV and access control systems, communications systems, remote access systems,**[** trading platforms,**]** email and instant messaging systems,	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel**[** and with consultants we may engage**]**

	intranet and Internet facilities, telephones, voicemail, mobile phone records [*insert any other relevant systems such as data loss prevention tools, next-generation firewalls, unified threat management systems, transport layer security, eDiscovery technology, mobile device management systems*]	access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with **[**for security vetting and investigating complaints and allegations of criminal offences**]** **[**for statistical analysis**]** to prevent unauthorised access and modifications to our systems as part of investigations by	For further information, see ****** below

		regulatory bodies, or in connection with legal proceedings or requests	
Details of your use of business-related social media, such as LinkedIn	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]** For further information, see ****** below

		covenants) are being complied with **[**for security vetting and investigating complaints and allegations of criminal offences**]** as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Your use of public social media (only in very limited circumstances, to check specific risks for specific functions within our organisation; you will be notified separately if this is to occur)	From relevant websites and applications	Legitimate interests: to monitor and manage staff access to our systems and facilities to protect our networks, and personal data of employees and customers/clients, against unauthorised access or data leakage to ensure our business policies, such as those concerning security and internet use, are adhered to for operational reasons, such as maintaining employment records, recording transactions, training and quality control to ensure that	To protect and carry out our legitimate interests (see adjacent column) Information shared with relevant managers, HR personnel **[**and with consultants we may engage**]** For further information, see ****** below

		commercially sensitive information is kept confidential to check that restrictions on your activities that apply after your employment has ended (post-termination restrictions or restrictive covenants) are being complied with **[**for security vetting and investigating complaints and allegations of criminal offences**]** as part of investigations by regulatory bodies, or in connection with legal proceedings or requests	
Details in references about you that we give to others	From your personnel records, our other employees	To perform the employment contract To comply with our legal obligations Legitimate interests: to maintain employment records and to comply with legal, regulatory and corporate governance obligations and good employment practice	To provide you with the relevant reference To comply with legal/regulatory obligations Information shared with relevant managers, HR personnel and the recipient(s) of the reference

You are required (by law or under the terms of your contract of employment, or in order to enter into your contract of employment) to provide the categories of information marked '☐' above to us to enable us to verify your right to work and suitability for the position, to pay you, to provide you with your contractual benefits, and to administer statutory payments such as statutory sick pay (SSP). If you do not provide this information, we may not be able to employ you, to make these payments or provide these benefits.

***** Further details on how we handle sensitive personal information **[**and information relating to criminal convictions and offencesare set out in our employee privacy notice, or for further information please refer to your DPO or Office Manager****** Further information on the monitoring we undertake in the workplace and how we do this is, please request to speak with our Data Protection Officer.

Appendix 1

Disability Nottinghamshire
Data Protection Impact Assessment (DPIA)

This DPIA should be used for changes to projects and systems.

To be completed by the Project Manager or person for the information will be collected or used differently. They will need to work with others who are delivering the work.

You should think about privacy and data protection at the start of the project or change. You need to know what you want to achieve, but complete this form as part of the startup phase so it can influence the design.

1) Explain what the project or change aims to achieve, what the benefits will be to us, to individuals and to other parties. Please list all individuals involved. You may find it helpful to link to other relevant documents related to the project.
2) What are the risks or challenges identified?
3) What the lawful basis for processing this data is.

4) What security measures are in place to safely store this data?
5) Are there any risks identified with storage?
6) Please give a list of all people that will have access to the data and the need for the access. You should minimise access to the appropriate level for each role.
7) How will staff or volunteers know how to appropriately use the data?
8) List any 'special categories' of data this will involve processing.
9) For all risks identified, specify additional measures to be put in place to minimise risks and comply with GDPR requirements.

Signed……

Date……

Review Date…….

Appendix 2.

Disability Nottinghamshire
Legitimate Interest Assessment

This legitimate interest assessment (LIA) template is designed to help you to decide whether or not the legitimate interest basis is likely to apply to your processing (This would usually be done when explicit consent is not appropriate).

If you want to rely on legitimate interests, you can use the three-part test to assess whether it applies. We refer to this as a legitimate interest's assessment (LIA) and you should do it before you start the processing.
An LIA is a type of light-touch risk assessment based on the specific context and circumstances. It will help you ensure that your processing is lawful. Recording your LIA will also help you demonstrate compliance in line with your accountability obligations under Articles 5(2) and 24. In some cases an LIA will be quite short, but in others there will be more to consider.

1) Purpose of processing?

- Why do you want to process the data?
- What benefit do you expect to get from the processing?
- Do any third parties benefit from the processing?
- Are there any wider public benefits to the processing?
- How important are the benefits that you have identified?
- What would the impact be if you couldn't go ahead with the processing?
- Are you complying with any specific data protection rules that apply to your processing (eg profiling requirements or e-privacy legislation)?
- Are you complying with other relevant laws?
- Are you complying with industry guidelines or codes of practice?
- Are there any other ethical issues with the processing?

2) Necessity (You need to assess whether the processing is necessary for the purpose you have identified).

- Will this processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose?
- Can you achieve the same purpose without the processing?
- Can you achieve the same purpose by processing less data, or by processing the data in another more obvious or less intrusive way?

3. Balancing. (You need to consider the impact on individuals' interests and rights and freedoms and assess whether this overrides your legitimate interests).

- Is it special category data or criminal offence data?
- Is it data which people are likely to consider particularly 'private'?
- Are you processing children's data or data relating to other vulnerable people?
- Is the data about people in their personal or professional capacity?

4) Reasonable Expectations.

- Do you have an existing relationship with the individual?
- What's the nature of the relationship and how have you used data in the past?
- Did you collect the data directly from the individual? What did you tell them at the time?
- If you obtained the data from a third party, what did they tell the individuals about reuse by third parties for other purposes and does this cover you?
- How long ago did you collect the data? Are there any changes in technology or context since then that would affect expectations?
- Is your intended purpose and method widely understood?
- Are you intending to do anything new or innovative?
- Do you have any evidence about expectations – e.g. from market research, focus groups or other forms of consultation?
- Are there any other factors in the particular circumstances that mean they would or would not expect the processing?

5) Likely Impact

- What are the possible impacts of the processing on people?
- Will individuals lose any control over the use of their personal data?
- What is the likelihood and severity of any potential impact?
- Are some people likely to object to the processing or find it intrusive?
- Would you be happy to explain the processing to individuals?
- Can you adopt any safeguards to minimise the impact?

Can you rely on legitimate interest for this processing? Yes / No

Give justifications for decision

Signed ……..

Date……..

Review Date……

Appendix 3
Employee/ volunteer Letter template

[*Date*]

[*State how delivered*: e.g. By Hand OR By 1st Class and Registered Post]
PRIVATE & CONFIDENTIAL
[*Name/address*]

Private and confidential

Dear [*insert name*]

New data protection privacy notices

Further to [*set out details of the action that the employer has already taken in order to effectively launch the new notices, eg information sessions, training etc*], I enclose a data protection privacy notice. Please read the notice carefully and keep it in a safe place as it contains important information about:

- who collects personal information about you;
- which information we collect and how and why we do so;
- how we use the information and who we may share it with;
- **[**any monitoring we undertake;**]**
- where we may hold your personal information**[** (including details of any international transfers of it)**]**;
- how long we keep your information;
- your rights to correct and access your information and to ask for it to be erased;
- details of where you can find further information about some of the matters listed above; and
- how to complain if we get things wrong and cannot resolve them for you.

[As discussed[*refer to the information session, training etc*], the OR The**]** reason we are sending you this new notice is to make sure we comply with new legislation governing data protection, known as the General Data Protection Regulation or 'GDPR' and the legislation proposed in the Data Protection Bill. We are not making any significant changes to the way in which we process information or the reasons for which we do so, but we are being even more open and transparent about what we do with the information we hold and process about you.

As a consequence of the new legislation, we will no longer be relying on your general 'consent' to us processing your personal information as a legitimate basis on which to undertake that processing. **[If there is a consent clause in the individual's contract:** This means that, from **[**the date of this letter OR 25 May 2018**]** we will no longer seek to rely on [*set out, as precisely as possible, details of the relevant consent provision, eg 'clause X of your contract of employment dated X'*].**]**

We may, however, seek your consent by other means to process your personal information at other times. For example, we will typically seek your consent before we process personal information in order to obtain a medical report about your health.

We wish to maintain our open and transparent approach in relation to the protection of personal information. Please therefore do not hesitate to contact **[**our Data Protection Officer [*insert name*] OR [*insert name*]**]** [*insert details of how DPO/named contact can be contacted*], who will be pleased to help with any queries you might have.

Yours sincerely

[*CEO/Other senior person*]

Appendix 4.
Privacy Notice letter template

[*Date*]

[*State how delivered*: e.g. By Hand OR By 1st Class and Registered Post]
PRIVATE & CONFIDENTIAL
[*Name/address*]

Private and confidential

Dear [*insert name*]

New data protection privacy notices

I enclose a data protection privacy notice. Please read the notice carefully and keep it in a safe place as it contains important information about:

- who collects personal information about you;
- which information we collect and how and why we do so;
- how we use the information and who we may share it with;
- where we may hold your personal information;
- how long we keep your information;
- your rights to correct and access your information and to ask for it to be erased;
- details of where you can find further information about some of the matters listed above; and
- how to complain if we get things wrong and cannot resolve them for you.

We are sending you this new notice to make sure we comply with new legislation governing data protection, known as the General Data Protection Regulation or 'GDPR' and the legislation proposed in the Data Protection Bill.

Please therefore do not hesitate to contact **[**our Data Protection Officer [*insert name*] OR [*insert name*]**]** [*insert details of how DPO/named contact can be contacted*], who will be pleased to help with any queries you might have.

Yours sincerely

[*CEO/Other senior person*]

Appendix 5.

Disability Nottinghamshire
Privacy Notice (Easy Read format).

(Pending completion. May 2018)

To Read for telephone enquiries, but can be used for face to face enquiries.

"Before we continue, I may need to collect some personal information from you, so we can best help with your enquiry."

"I need to ask for ***your permission to record and use the personal information you give me. We can still help with your enquiry if you don't want to give us your permission,*** *but it might limit us in what we can do to help."*

"You may have heard, all businesses in the UK have to follow new data protection laws, which include making sure that you are aware of both your rights and how we, as an organisation, use your data .Of course ***we comply with all the laws about data protection, and keep your personal information confidential, safe and secure.*** *I* ***can provide you with more information about how we do this****, right now over the phone, or if you prefer I can send it to you, or show you where you can find it on our website."*

"How would you like to proceed?"

"Would you like me to read it to you just now?"

IF YES.

"No problem at all, this will just take a couple of minutes."(Go to page 2).

CONTINUE TO READ PRIVACY NOTICE & RECORD HAS BEEN READ. ***RECORD CONSENT.***
Or

RECORD CONSENT *& AND ANY REQUEST TO FORWARD NOTICE.*
Or

RECORD CONSENT *& DIRECT TO WEBSITE.*
Or

RECORD THAT CONSENT HAS NOT BEEN GIVEN*, BUT CONTINUE WITH ENQUIRY WITHOUT RECORDING PERSONAL DETAILS.*
"Thanks for that. Now, how can I help you?"

This is an example of our privacy notice read out on telephone.

"Your personal details that we discuss today are stored and used by Disability Nottinghamshire. We use your data based on the consent, or permission that you provided to us, and we won't share it with anyone else, without your express permission, unless we have a legal obligation to do so."

"We will only use your personal information to help provide you with the best service, to monitor the quality of our service, and help provide statistics for funding purposes. These statistics would never identify you personally. All your personal details are kept secure and confidential."

"For any enquiries specifically regarding data we store about you, or how Disability Nottinghamshire uses your data, you can contact our Data Protection Officer via e-mail at or write to them at our company address marking your letter for the attention of the Data Protection Officer.
"If at any point you wish to see a copy of the data we hold on you, details of how we use and store your data, or receive further details regarding your rights, you can request this from us via phone or e-mail .

"Would you like me to provide our contact details?"

"If any data we hold regarding you is incorrect, you may request a correction to your data at any time."

"You may also request that we cease processing your data at any time or to object to our continued use of your data.

"You also have the right to request that we delete any or all personal data we hold about you. The only reason we would not carry out this request is if it would result in us being in breach of other legal or regulatory obligations we have, but we would always inform you at the time were this the case."

"If for any reason you are unhappy, you can lodge a complaint with us, or you can contact the Information Commissioner's Office using their website at ico.org.uk by clicking the "Report a concern" link and then following the steps found on the page."